PATENT CLAIMS

1. Method of producing electronic security elements, in particular chip cards, comprising the following method steps:

1.1 at least one test value, in particular a public key of the purchaser of the chip card, is stored in a memory area of the chip during chip manufacture,

1.2 during initialization of the electronic security element use is made of an optionally addressable test value,

1.3 the authenticity of data introduced during the initialization is checked with the aid of the test value stored in the chip card,

1.4 the initialization is terminated in the event of a negative outcome of the check.

2. Method according to Claim 1, in which, instead of the public key of the purchaser of the chip card, a hash value derived therefrom is introduced into the memory area of the chip.

3. Method according to any of the preceding claims, in which the public key and/or the hash value is generated by the purchaser of the chip card and the manufacturer of the chip and/or of the ROM mask is informed thereof.

4. Method according to Claim 3, in which the algorithm used to calculate the hash value is given to the manufacturer of the chip and/or of the ROM mask and is also stored in the memory of the chip.

5. Method according to Claim 2 or 3, in which the hash value is generated by the manufacturer of the chip and/or of the ROM mask and is stored in the memory of the chip together with the algorithm used to generate it.

6. Method according to any of Claims 1 to 5, in which the hash value of the input public key is recalculated using the algorithm and the result is compared with the stored hash value.

7. Method according to any of the preceding claims, in which, during the initialization, the public key or hash value and the algorithm used to generate the hash value are specified.

8. Method according to any of the preceding claims, in which, if there are a number of possible purchasers of the chip card, a public key or hash value and/or the algorithm for generating it is stored for each purchaser.

9. Method according to any of the preceding claims, in which a number of public keys or hash values for a number of public and/or secret keys are stored for a purchaser of the card.

10. Security module, containing a chip comprising a ROM mask and an EEPROM, wherein a hash value of the public key of the purchaser of the chip card or the public key itself is stored in the ROM, and the operating system is designed in such a way that initialization is possible only in the event of a successful signature check using the public key of the purchaser of the chip card.

11. Security module according to Claim 10, in which details regarding the algorithm used to calculate the hash value are also stored in the ROM.

12. Security module according to Claim 10 or 11, in which, if there are a number of possible purchasers of the chip card, a hash value and/or an algorithm for generating it is stored for each purchaser.

13. Security module according to any of Claims 10 to 12, in which a number of public keys or hash values for a number of public keys are stored for a purchaser of the card.